

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-85493

(P 2 0 0 3 - 8 5 4 9 3 A)

(43) 公開日 平成15年3月20日 (2003. 3. 20)

(51) Int. Cl. ⁷	識別記号	F I	テマコード (参考)
G06K 17/00		G06K 17/00	L 2C005
B42D 15/10	521	B42D 15/10	521 5B017
G06F 12/00	537	G06F 12/00	537 D 5B058
12/14	310	12/14	310 K 5B075
	320		320 A 5B082

審査請求 未請求 請求項の数 3 O L (全13頁) 最終頁に続く

(21) 出願番号 特願2001-273543 (P 2001-273543)

(22) 出願日 平成13年9月10日 (2001. 9. 10)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 林 良一

東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

(72) 発明者 ▲高▼倉 健

東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

(74) 代理人 100069981

弁理士 吉田 精孝

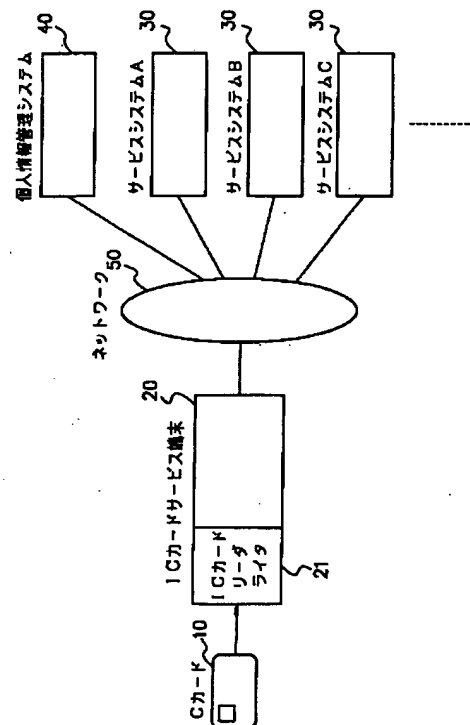
最終頁に続く

(54) 【発明の名称】 個人情報統合管理システム及びそのプログラム並びにそのプログラムを記録した媒体

(57) 【要約】

【課題】 複数のサービスシステムの情報連携によってユーザの意図しない個人情報が作り出されることがない個人情報統合管理システムを提供すること。

【解決手段】 ICカード10にサービスシステム30毎の顧客認証に用いる鍵ペアを用意しておき、サービスシステム30に公開鍵を送信する。サービスシステム30ではユーザ用に作成した顧客IDと受信した公開鍵に対しサービスシステム固有の暗号鍵により署名を行った電子証明書を作成し、ICカード10に送信する。サービスシステム30から個人情報管理システム40に情報連携処理要求があると、個人情報管理システム40はサービスシステムIDと顧客IDとからデータベースを検索し、ユーザIDを特定し、該ユーザIDの個人情報と関連付ける。ユーザが匿名でサービスを受けるための識別情報をサービスシステム毎に個別に用意することで、プライバシーを侵害するような情報連携を避ける。



【特許請求の範囲】

【請求項 1】 少なくともユーザの個人情報を格納した IC カードと、IC カードとの間でデータを送受信するための IC カードリーダライタを有する IC カードサービス端末と、IC カードに IC カード用アプリケーションプログラムを提供するとともに IC カードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動した IC カード及び IC カードサービス端末を通じてユーザにサービスを提供する複数の IC カードサービスシステムであってそのうちの少なくとも 1 つは IC カードに格納されたユーザの個人情報を利用してユーザにサービスを提供する複数の IC カードサービスシステムと、IC カードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムと、IC カードサービス端末と複数の IC カードサービスシステムと個人情報管理システムとを接続するネットワークとからなり、前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有する個人情報統合管理システムにおいて、前記情報連携機能は、

IC カードに格納された個人情報を、ユーザ ID を含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、

サービスシステムにおいて顧客 ID と電子証明書とを作成し、サービスシステム ID と顧客 ID と証明書とを IC カードに格納し、サービスシステム ID と顧客 ID とを個人情報管理システムに格納する第二の事前処理ステップと、

IC カードからサービスシステムに証明書を送信するサービス利用ステップと、

サービスシステムから個人情報管理システムに顧客情報とサービスシステム ID と顧客 ID とを送信する第一の連携処理ステップと、

個人情報管理システムにおいてサービスシステム ID と顧客 ID とを用いて個人情報データベースからユーザ ID を特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザ ID を用いて個人情報データベースから該ユーザ ID に対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって実現されることを特徴とする個人情報統合管理システム。

【請求項 2】 少なくともユーザの個人情報を格納した IC カードと、IC カードとの間でデータを送受信するための IC カードリーダライタを有する IC カードサー

ビス端末と、IC カードに IC カード用アプリケーションプログラムを提供するとともに IC カードサービス端末に端末用アプリケーションプログラムを提供し、各アプリケーションプログラムが起動した IC カード及び IC カードサービス端末を通じてユーザにサービスを提供する複数の IC カードサービスシステムであってそのうちの少なくとも 1 つは IC カードに格納されたユーザの個人情報を利用してユーザにサービスを提供する複数の IC カードサービスシステムと、IC カードに格納されたユーザの個人情報を管理するサービスを提供する個人情報管理システムと、IC カードサービス端末と複数の IC カードサービスシステムと個人情報管理システムとを接続するネットワークとからなり、前記個人情報管理システムは、前記サービスシステムの要求に基づき、該サービスシステムの顧客情報と、該個人情報管理システムの個人情報とを結び付け、結び付けた連携情報は、該個人情報の利用条件情報と、該サービスシステムのサービスシステム情報から個人情報管理システムが許可した内容とによる利用制御に基づいた提供がなされる情報連携機能を有する個人情報統合管理システムのプログラムであって、

該プログラムはコンピュータ上に、

IC カードに格納された個人情報を、ユーザ ID を含む形で個人情報管理システムの個人情報データベースに格納する第一の事前処理ステップと、

サービスシステムにおいて顧客 ID と電子証明書とを作成し、サービスシステム ID と顧客 ID と証明書とを IC カードに格納し、サービスシステム ID と顧客 ID とを個人情報管理システムに格納する第二の事前処理ステップと、

IC カードからサービスシステムに証明書を送信するサービス利用ステップと、

サービスシステムから個人情報管理システムに顧客情報とサービスシステム ID と顧客 ID とを送信する第一の連携処理ステップと、

個人情報管理システムにおいてサービスシステム ID と顧客 ID とを用いて個人情報データベースからユーザ ID を特定する第二の連携処理ステップと、

個人情報管理システムにおいてユーザ ID を用いて個人情報データベースから該ユーザ ID に対応する個人情報を検索し、顧客情報と検索から得られた個人情報とを連携付ける第三の連携処理ステップとを含む処理によって前記情報連携機能を実現することを特徴とする個人情報統合管理システムのプログラム。

【請求項 3】 請求項 2 に記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、複数の IC カードサービスシステムで使用されるユーザの個人情報を、ユ

10

20

30

40

50

ーザ自身が主体的に管理し、かつ IC カードサービスシステムに必要な個人情報の使用をユーザが設定した利用条件に基づいて制御する、個人情報統合管理システムを実現するための技術に関する。

【0002】

【従来の技術】従来、サービスの提供者が、サービス利用履歴や趣味・嗜好等のユーザの個人情報を管理し、これをユーザに対するマーケティングに活用するケースが数多く見受けられていた。

【0003】近年は、IC カードを用いた IC カードサービスシステムを構築して、ユーザ情報の管理を行うシステムが増加している。これは、耐タンパ性に優れた IC カードの安全性を活用しようというもので、課金・決裁・資産管理サービスのような金銭の出納に関わるサービスや、電子行政・医療情報システムなど、繊細な情報やプライバシーに関わる情報を扱うサービスに対し、暗号・認証技術を用いた堅牢なユーザ認証を実現するために導入されたものである。

【0004】IC カードは、従来の磁気カードと比べ高コストであることから、複数の IC カードサービスシステムを 1 枚のカードで共用できるような高機能性が求められていたが、最近の IC チップの演算能力と記憶容量の向上に伴い、1 枚の IC カードに複数のアプリケーション処理プログラムを搭載することができるようになった。これに併せ、IC カードに搭載するアプリケーションについても、共通の開発環境と実行環境を提供するプラットフォームが開発されている（例えば、NTT 技術ジャーナル、2000 年 10 月号、p. 15-18、p. 56-59 参照）。

【0005】IC カードサービスシステム開発の現状を見ると、IC カード媒体の特徴である携帯性と安全性を活かしたシステム構築がなされてはいるものの、IC チップの演算処理能力を応用した高機能性の十分な活用には至っていないようである。

【0006】具体的には、これまでの IC カードサービスシステムでは、IC カードから IC カードサービスシステムにデータベース処理言語である SQL コマンドを送信することで、IC カードサービスシステムの個人情報データベースに対する処理を実行する等、IC カードに単なる情報蓄積媒体以上の機能を発揮させていた。

【0007】しかし、IC カード上での処理は、IC カードに蓄積されていた該 IC カードサービスシステム向けに用意された処理プログラムとパラメータが選択され起動されるというものであり、高機能 IC カードサービスシステムの使い道としては比較的容易な処理内容に過ぎなかった。

【0008】一方、IC カードサービスシステムで利用される個人情報については、上述したように、従来からマーケティングに役立つ情報として認められていたが、近年の通信ネットワークの普及に伴う電子サービスの

て、電子化された個人情報をを用いることで容易に実現されるようになったマス・カスタマイゼーションが、マーケティング戦略面のみならず、効率面でも有効であることが判明すると、特に電子化された個人情報の価値はますます増大してきた。事実、通信ネットワーク上でのサービス提供企業が売却される際に、該企業の有する個人情報重要な資産価値として認められもしている。

【0009】しかしながら、個人情報が電子化され通信ネットワーク上で利用されることには、ユーザとして安全面での懸念がある。セキュリティ、プライバシーの問題がそれである。個人情報保護に関する法律制定の動きもあるが、ユーザも自己防衛を考えるようになり、また、サービス提供者としても信用問題につながるため、相当の力を入れるようになってきつつある。

【0010】通信ネットワークにおける個人情報流通を技術面から支えるため、暗号・認証やデータ利用制御技術が開発され、後者においては、ユーザがユーザ自身の個人情報に利用条件を課す方法が考案されている（例えば、寺西裕一 他「利用規約に基づくマルチメディアコンテンツ流通システムの設計」情処研報 99-DPS-95、Vol. 99、No. 94、1999、pp 31-36 参照）。これは、個人情報の管理に対しユーザが主導権を持つことにつながり、また、個人情報が通信ネットワーク上を流通する世界を想定したものでもある。

【0011】

【発明が解決しようとする課題】このような状況の下、多数の IC カードサービスシステム導入の動きがあるが、現状のまま IC カードサービスシステムの構築が進められると、ユーザの個人情報が複数の IC カードサービスシステムで独立に存在し、各 IC カードサービスシステムで管理されることになる。すると、ユーザの個人情報は各 IC カードサービスシステムで管理され、IC カードサービスシステムの数だけ存在することになるので、ユーザは利用したいシステムの数だけ IC カードを携帯する必要が生じ、ユーザ自身の個人情報であるにも拘わらず、ユーザ自身で管理することができず、ユーザの個人情報に何らかの変更が生じた場合、複数のシステムに対してそれぞれ個人情報更新処理を行わなければならない。また、ユーザはユーザ自身の個人情報がどこでどのように使用されているか把握できず、個人情報がユーザの意図に沿わない使われ方をされる可能性がある。また、派生的課題として、IC カードサービスシステム間で個人情報を流通する際に、ユーザが予想していないシステム間の情報連携により、個人のプライバシーに関わる情報が生じる危険がある。

【0012】そこで、本発明では、IC カードサービスシステム毎に管理されているユーザの個人情報を、ユーザ自身が管理できるようにし、各 IC カードサービスシステムが必要とする個人情報をユーザが許可した条件の下でのみ利用可能とし、IC カードサービスシステムに

提供した個人情報の使われ方を制御でき、特に、複数のＩＣカードサービスシステムの情報連携によってユーザの意図しない個人情報が作り出されることがない個人情報統合管理システムを提供することを目的とする。

【0013】

【課題を解決するための手段】上記の課題を解決するために、本発明では、ＩＣカードの多機能性を従来以上に発揮させ、１枚のＩＣカードに複数のサービス処理機能を持たせてワンカード化を図り、また、暗号・認証技術と利用制御技術を利用して、個人情報の安全な流通の仕組みを設ける。そして、ＩＣカードと複数のＩＣカードサービスシステムが相互に情報連携しての処理が可能となるＩＣカードサービス環境を構築する。

【0014】具体的には、ＩＣカード上に、個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のＩＣカードサービスシステムのＩＣカードにおける処理プログラム（カード用サービスＡＰ）及びこれに用いる情報（ＡＰ個人情報）を、複数サービス分だけ搭載する。この時、ＩＣカードサービスシステムの１つとして、ユーザの個人情報を管理するサービスを行う個人情報管理システムを用意し、該システムのＩＣカードにおける処理プログラム（カード用管理ＡＰ）をＩＣカードに搭載しておく。

【0015】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び通常各ＩＣカードサービスシステム（以下、サービスシステムと略す）のＡＰ個人情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービスとして提供する。また、個人情報管理システムは、サービスシステム情報を管理する機能を有する。そして、あるサービスシステムに対する個人情報を利用した処理においては、該サービスシステムに対応するサービスシステム情報と個人ＡＰ情報を参照することで、個人情報の利用制御や、情報連携サービスや、カード用サービスＡＰの処理制御を行う。

【0016】一方、システム間での情報連携が個人のプライバシーを侵害するのを防ぐために、サービスシステムの顧客情報と、管理システムの個人情報を匿名のまま関連付ける仕組みを設ける。

【0017】個人情報管理システムにおけるユーザ認証や、サービスシステムにおける顧客認証には、公開鍵暗号方式を用いたチャレンジ&レスポンスによる認証を用いる。

【0018】ＩＣカードには、サービスシステムの顧客認証に用いる鍵ペアを用意しておき、サービスシステムに公開鍵を送信する。

【0019】サービスシステムでは、ユーザ用に作成した顧客ＩＤと受信した公開鍵に対しサービスシステム固有の暗号鍵により署名を行った電子証明書（以下、証明

書）を作成し、ＩＣカードに送信する。

【0020】個人情報管理システムでは、サービスシステムＩＤと顧客ＩＤとからユーザＩＤを検索できるようなデータベースを構築する。

【0021】

【作用】本発明の個人情報統合管理システムは、個人情報管理サービスを提供する個人情報管理システムと、各種サービスを提供する複数のサービスシステムと、カードリーダライタが付属したＩＣカードサービス端末と、そして、各ユーザの個人情報等を蓄積したＩＣカードにより構成される。ＩＣカード上には、個人情報管理システムで管理する個人情報と該個人情報の利用条件情報とを蓄積し、更に、複数のサービスシステムのカード用サービスＡＰ及びＡＰ個人情報を搭載する。

【0022】個人情報統合管理システムでは、ＩＣカードサービスシステムの１つとして個人情報管理システムを用意し、ユーザの個人情報を管理するサービスを行う。個人情報管理サービスを利用するには、ＩＣカードサービス端末で、カード用個人情報管理ＡＰ（カード用管理ＡＰ）をＩＣカードに予めダウンロードする。そして、ユーザはＩＣカードサービス端末（カード端末）で個人情報管理サービスのクライアントプログラム（端末用管理ＡＰ）を起動する。

【0023】個人情報管理システムは、複数のユーザの個人情報及び各個人情報に課した利用条件情報及び各サービスシステムの個人ＡＰ情報を各ユーザが主体となって管理する機能と、各ユーザの個人情報を各ユーザの利用条件情報に基づいて制御する機能を、個人情報管理システムのサービス（管理サービス）として提供する。

【0024】ユーザが各サービスシステムのサービスを利用するには、カード端末で、利用する各サービスシステムのカード用サービスＡＰを予めＩＣカードにダウンロードする。そして、ユーザはＩＣカードサービス端末（カード端末）で利用したいサービスシステムのクライアントプログラム（端末用サービスＡＰ）を起動する。端末用サービスＡＰは、カード用管理ＡＰが管理する個人情報及び利用条件情報と、カード用サービスＡＰが管理する個人ＡＰ情報を利用して、各サービスシステムが提供する様々な処理を行う。

【0025】個人情報管理システムの管理サービスは、サービスシステムの個人情報要求に対し、ユーザが設定した個人情報と利用条件情報とを用い、ユーザが許可した範囲で個人情報を提供する。ＩＣカードがシステムに接続されていない場合も、管理サービスは利用条件付き個人情報を提供できる。

【0026】個人情報管理システムとサービスシステムとの情報連携については、サービスシステムから個人情報管理システムに情報連携処理要求があると、個人情報管理システムはサービスシステムＩＤと顧客ＩＤとからデータベースを検索し、ユーザＩＤを特定し、該ユーザ

IDの個人情報と関連付ける。この関連付け処理では、ユーザIDをシステム処理の工程内でのみ使用しているので、結果を抽出する前に利用条件に基づく利用制御を行うことで、プライバシーを侵害するような情報連携を避けることができる。

【0027】

【発明の実施の形態】本発明の個人情報統合管理システムの実施の形態の一構成例について、図1を用いて説明する。

【0028】図1において、10はICカード、20はICカードサービス端末（以下、カード端末と略す）、30は複数の通常のICカードサービスシステム（以下、サービスシステムと略す）、40は個人情報管理システム、50はネットワークである。

【0029】本発明の個人情報統合管理システムでは、カード端末20と、複数のサービスシステム30と、個人情報管理システム40とがネットワーク50を介して接続されている。これらに加え、各ユーザのICカード10が、単体では機能しないが、カード端末20のICカードリーダライタ（ICカードRW）21に挿入されることでシステムの一部として動作する。

【0030】更に、システムには、ユーザが初めてICカードサービス環境である個人情報統合管理システムにアクセスしようとする際に、該ユーザに初期情報を記録したICカードを発行する個人情報登録システムが接続されていても良い。本発明ではこの個人情報登録システムを必須の構成要素とはしないが、個人情報統合管理システムの中で絶対の信頼機関として個人情報登録システムを使用する構成も可能である。

【0031】いずれにせよ、本システムでは、それぞれが通信を行うために信頼関係を保たなければならないので、接続の際に相互認証を行う。具体的には、ICカード10はカード端末20に挿入する際に、また、カード端末20とサービスシステム30と個人情報管理システム40とはネットワーク50で接続する際に相互認証を行う。

【0032】相互認証には、個人情報登録システムなどにおいて発行された証明書を用い、公開鍵暗号方式を用いたチャレンジ&レスポンスにより互いに認証することで相互認証を行う。

【0033】証明書は、申請者が作成した鍵ペアの公開鍵及び登録システムが発行したIDに対し、登録システム固有の暗号鍵により署名を行うことにより作成する。

【0034】これら個人情報統合管理システムを構成する各構成要素が格納・管理している情報を図2に示す。項目に記した具体的なプロパティは、情報のカテゴリを分かり易く示すための例である。また、ICカードは記憶容量に制限があるので、カード用管理アプリケーションプログラム（AP）で蓄積するデータはポインタとして機能する情報であっても良い。

【0035】ICカード10にはユーザの個人情報が格納されている。個人情報には、ユーザを特定する又はユーザを特徴づけるための住所、氏名、年齢、性別、趣味、嗜好……といった情報等の基本情報と、各サービスシステムのアプリケーションを利用する際に必要なサービスシステム用個人情報と、個人情報管理システム及び各サービスシステムを介して利用してきたログ情報である個人履歴情報と、そして、これら基本情報・サービスシステム用個人情報・個人履歴情報の個々の項目についての利用条件を定めた利用条件情報とがある。

【0036】サービスシステム30には、サービスシステム情報と、顧客情報とが格納されている。サービスシステム情報は、該サービスシステムが主体となって管理する、サービスシステムを特定・識別する又はサービスシステムの特徴を示す情報である。顧客情報は、該サービスシステムが主体となって管理する、サービスシステム利用ユーザ毎に取得した情報である。

【0037】個人情報管理システム40では、ユーザが主体となって管理している、ICカードに格納する個人情報の全て又は個人情報に課せられた利用条件情報が個人情報管理システムに許す範囲の個人情報を格納している。加えて、サービスシステムが主体となって管理しているサービスシステム情報を、各サービスシステムの分だけ管理している。

【0038】個人情報統合管理システムを利用しようとするユーザは、ユーザ自身の個人情報を管理するために、個人情報管理システム40の個人情報管理サービス（管理サービス）を使用する。ICカード情報を可視化し、情報を操作するソフトウェアがあれば管理はできるが、ICカード情報をオンラインで扱うためには、個人情報管理システムが必要になる。

【0039】個人情報管理サービスの概要を図3及び図4を用いて説明する。

【0040】図3は個人情報管理システムの概要を示すもので、図中、41は個人情報データベース、42はサービスシステムデータベース、43は個人情報管理モジュール、44はサービスシステム管理モジュール、45は利用制御モジュールである。また、図4は個人情報管理サービスの処理の流れを示す。

【0041】初めて個人情報管理システム40にアクセスするユーザは、予めカード端末20でICカード10にカード用個人情報管理AP（以下、カード用管理APと略す）11をダウンロードする。そして、管理サービスを利用する場合、ユーザはカード端末20で端末用個人情報管理AP（以下、端末用管理APと略す）22を起動し、カード端末20のICカードRW21に挿入したICカード10上のカード用管理AP11を用いて、個人情報及び各個人情報に対する利用条件の設定など、個人情報管理の操作を行う。

【0042】ユーザは、管理サービスを利用して設定し

た個人情報及び利用条件情報の原本を、ICカード10上のカード用管理AP11に保存する。個人情報管理システム40の個人情報管理モジュール43では、カード用管理AP11の個人情報と利用条件情報を、管理システム40に対し定めた利用条件の範囲で個人情報管理システム40の個人情報DB41に保存する。個人情報管理システム40に対して定める個人情報の利用条件としては、個人情報の全てを取り扱うことができるように特権システムとして定めることが望ましいが、必要ならば適当な利用条件を定めることで利用制御させることも可能である。

【0043】尚、個人情報管理システム40中、サービスシステムDB42、サービスシステム管理モジュール44及び利用制御モジュール45については、図7、8を用いて後ほど説明することとし、管理サービスの処理の流れを説明する。

【0044】カード端末20で端末用管理AP22を起動しておき、そこにICカード10が挿入されるとICカード10上のカード用管理AP11が起動され、管理サービスが可能になる。カード用管理AP11は、本管理サービスのサービス認証を行い、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【0045】一方、個人情報管理システム40の個人情報管理モジュール43は、ICカード利用者のユーザ認証を行い、システム上の個人情報DB41から利用条件を判断しながら個人情報の読み出しを行う。これらの個人情報は端末用管理AP22に送信され、具体的なユーザの管理操作を受け付ける管理サービスが提供される。

【0046】ユーザがカード端末20で個人情報操作の管理サービス処理を行うと、処理内容に応じ、ICカード10または個人情報管理システム40に処理内容が送信、処理される。処理が終わればカード端末20に処理完了の通知が返り、ICカード10上のカード用管理AP11が終了し、カード端末20での操作に従い、ICカード10が排出される。

【0047】次に、サービスシステムによる提供サービスの概要を図5及び図6を用いて説明する。

【0048】図5はサービスシステムの概要を示すもので、図中、31はサービスシステム顧客データベース、32はサービス処理モジュールである。また、図6はサービスシステムにおける提供サービスの処理の流れを示す。

【0049】初めてサービスシステム30にアクセスするユーザは、カード用管理AP11に加え、カード用サービスAP12をICカード10に搭載しておく必要があり、予めカード端末20で該サービスのカード用サービスAP12をICカード10にダウンロードしておく。

【0050】サービスシステム30のサービスを受ける

には、カード端末20で端末用サービスAP23を起動する。この時、既にICカード10に搭載されているカード用管理AP11で保存している個人情報が、サービスに対し定められた利用条件情報の下で利用可能になる。端末用サービスAP23は、必要に応じてICカード10上のカード用サービスAP12及びカード用管理AP11と連携して、必要な個人情報を該サービスに課せられた利用条件情報に基づき利用しつつ、該サービスのサービス処理を遂行する。

【0051】サービスシステム30では、サービス処理モジュール32を介し、カード用管理AP11によって利用制御された個人情報をを用いてサービス処理が行われ、サービスシステム30が自身で収集したユーザ情報を顧客情報として収集する。

【0052】サービスシステム30の処理の流れとしては、まず、カード端末20で端末用サービスAP23を起動しておき、そこにICカード10を挿入する。サービスシステム30では、ICカード利用者の顧客認証を行い、サービスシステム30に格納されているサービスシステム情報を読み出す。ICカード10では、カード用サービスAP12の前にカード用管理AP11が起動される。カード用管理AP11はサービスシステム情報を参照し、利用しようとしているサービスシステム30の認証を行う。そして、該サービスに対する利用条件を判断の上、開示制御を加えた個人情報の読み出しを行う。

【0053】ICカード10上で動作するAPの制約から、APの複数起動が可能な場合と不可能な場合とがある。図6の例では、カード用管理AP11とカード用サービスAP12の双方のAPが同時に起動しないと仮定して、カード用管理AP11を終了させた後、カード用サービスAP12を起動している。

【0054】カード用サービスAP12の起動を受けて、端末用サービスAP11はICカード10からサービスに用いる情報の読み出しを行い、また、サービスシステム30からは顧客DB31から顧客情報の読み出しを行う。これらの情報は端末用サービスAP23に送信され、具体的なユーザの操作を受け付けるサービス提供が開始される。ユーザがカード端末20でサービス操作を行うと、処理内容に応じ、ICカード10またはサービスシステム30に処理内容が送信、処理される。

【0055】ICカード10とサービスシステム30での各々の処理の結果、必要に応じてICカード10または顧客DB31に処理情報の書き込みが行われる。処理が終わればカード端末20に処理完了の通知が返り、ICカード10上のカード用サービスAP12が終了し、カード端末20での操作に従い、ICカード10が排出される。

【0056】次に、個人情報管理システムの個人情報DBとサービスシステムの顧客情報DBとを連携させるサ

ービスについて図7及び図8を用いて説明する。図7は個人情報管理システム及びサービスシステムの概要を示す。また、図8は連携サービスの処理の流れを示す。

【0057】サービスシステム30は、ICカード10との接続を必要としない処理が目的で個人情報を扱おうとする場合や、統計処理などユーザー一般に関する情報を用いた処理を行う場合等に、個人情報管理システム40の管理サービスを利用する。サービスシステム30の顧客情報と個人情報管理システム40の個人情報を連携させるには、各データベースにユーザを特定するためのキーを設定しておく。この方法の詳細は図9を用いて別途説明する。

【0058】さて、個人情報管理システム40の個人情報管理サービスを利用するサービスシステム30は、個人情報管理システム40のサービスシステム管理モジュール44を介し、サービスシステムDB42にサービスシステム情報を登録しておく必要がある。サービスシステム情報の具体的な項目としては、サービスシステム毎に振られたサービスシステムID、サービスシステムの正当性を認証するための情報、サービスシステムの提供するサービスのカテゴリや特徴的キーワード等が挙げられる。

【0059】個人情報管理システム40は、サービスシステム30の要求に対しサービスシステム管理モジュール44でサービスシステムとしての認証等の処理を行い、利用制御モジュール45で該サービスシステム30の利用条件を判断し、許された範囲内で個人情報DB41から個人情報を抽出し、該個人情報をサービスシステム30に送信する。あるいは定められた利用条件によっては、逆に個人情報管理システム40で該情報を用いた

処理を行い、許可された結果のみをサービスシステム30に送信する。

【0060】個人情報管理システムとサービスシステムとの情報連携処理の流れとしては、まず、サービスシステム30から個人情報管理システム40へ、管理サービス利用のためのアクセス要求が送信される。管理システム40はアクセス要求したサービスシステム30の認証を行い、サービスシステムDB42からサービスシステム情報の読み出しを行う。

【0061】サービスシステム30は、更に、サービスシステム30で得られている顧客情報と個人情報に基づき、管理サービスの個人情報利用要求を送信する。すると管理システム40は、サービスシステム30の顧客IDに対応する個人情報との関連付けを行う。関連付けの方法は、先にも述べたように後述する。管理システム40は、関連付けられた個人情報を個人情報DB41から読み出し、該個人情報の利用条件を解析し、利用条件付き個人情報を生成する。サービスシステム30は、自ら所有する顧客情報に利用条件を設定して、これを管理システム40に送付する。

【0062】この時点で個人情報管理システム40にユーザに関する各種情報が取り揃えられたことになるが、個人情報管理システム40では、利用制御モジュール45において、個人情報と顧客情報を連携させ、連携情報に対しどのような利用条件情報を付与すれば良いかの解析を行う。そして、その判断に基づき、利用条件付きの連携情報が生成され、管理サービスの処理結果としてサービスシステム30に利用条件付き連携情報を引き渡す。

【0063】以上が一連の処理の流れであるが、利用条件に依っては、最後の工程で連携情報がサービスシステム30に引き渡されず、個人情報管理システム40上でのみ取り扱い可能な状態になることもある。このような時、もしもサービスシステム30に連携情報入手の許可は無くても、連携情報を使った別の処理が許可されていれば、個人情報管理システム40の利用制御モジュール45において処理が行われ、サービスシステム30に処理結果を返送することになる。

【0064】次に、ICカード10から個人情報管理システム40に送信され格納されている個人情報とサービスシステム30に格納されている顧客情報との連携サービスの実現例を図9を用いて説明する。ここでは、不要な個人情報の公開を防ぐため、匿名性を維持しつつ顧客情報に対応する連携先個人情報を判断する方法を例示する。

【0065】個人情報管理システム40には、ICカード10の個人情報、ユーザが設定した利用条件と共に格納されている(ステップ1-1)。次に、ICカード10またはカード端末20において鍵ペアを作成し、格納する(ステップ1-2)。

【0066】サービスを利用する際は、まず、公開鍵をサービスシステム30に送信する(ステップ2-1)。公開鍵を受信すると、サービスシステム30は顧客IDを発行し、顧客IDと公開鍵にサービスシステム固有の暗号鍵で署名を行うことにより証明書を作成する(ステップ2-2)。そして、ICカード10にサービスシステムIDと顧客IDと証明書とを格納し(ステップ2-3)、また、ユーザは個人情報管理システム40の個人情報DB41にサービスシステムIDと顧客IDとを格納しておく(ステップ2-4)。

【0067】ユーザがサービスシステム30のサービスを受ける際には、証明書をサービスシステム30に送信し、相互認証を行う。

【0068】サービスシステム30は、ユーザがサービスを利用する際にユーザから取得した顧客情報を、個人情報管理システム40の個人情報と連携させるために、まず、サービスシステム30から個人情報管理システム40にサービスシステムIDと顧客IDとを送信する(ステップ3-1)。

【0069】個人情報管理システム40では、サービス

システムIDと顧客IDとから個人情報DB41を検索し、ユーザIDを特定する(ステップ3-2)。得られたユーザIDを基に個人情報DB41を検索し、顧客情報と連携させるべき個人情報を得る(ステップ3-3)。

【0070】個人情報管理システム40の利用制御モジュール45は、サービスシステム30に許可された利用条件を判断し、サービスシステム30に提供を許された情報については利用制御を課したまま、個人情報管理システム40からサービスシステム30に送信する。サービスシステム30への該個人情報の提供は許されていないが、顧客情報と個人情報とを用いて行う何らかの処理の結果を知ることが許可されている場合、サービスシステム30から個人情報管理システム40へ該顧客情報を送信し、個人情報と連携させて実行した処理結果をサービスシステム30に返送する。

【0071】サービスシステム30が、個人情報の提供も個人情報を用いた処理の実行も許されていない場合、サービスシステム30から個人情報管理システム40への情報連携要求は不成功に終わる。

【0072】情報連携を用いた具体的な実施サービス例として、また、本発明の個人情報統合管理システムの発展的サービス例として、サービスシステムが顧客情報と個人情報との連携情報を統計情報として顧客動向調査に利用し、抽出した個人に対し広告を配送するサービスについて述べる。

【0073】あるサービスシステム(例えば、SS-Aとする)の顧客情報DBにサービス履歴情報を蓄積しておく。仮に、SS-Aが、SS-Aの提供するサービス甲を受けた顧客に特徴的な傾向を発見したとする。SS-Aは個人情報管理システム40と連携して、前記の特徴的な傾向を見せた顧客の顧客IDと、情報から関連付けられたユーザの個人情報を統計的に提供してもらう。

【0074】この時のユーザの利用条件では、例えば「母数100以上の統計処理への利用を許可」等の設定がなされている必要があり、そのような提供を許可していないユーザの個人情報は、統計情報としても提供されない。SS-Aは、情報連携で得られた統計情報の分析の結果、例えば「サービス甲を受け、引き続きサービス乙を利用する顧客は20代女性に多数見られる」等のマーケティング情報を得ることができる。

【0075】上記マーケティング情報を得たSS-Aは、サービス甲の利用ユーザの中でまだサービス乙を利用していない顧客に何らかの働きかけを行う、または広く一般ユーザに対して働きかけを行うと考えられる。その働きかけの手段として広告配送による方法がある。しかし、広告配送先である住所情報は、個人情報の1項目であり、SS-Aに公開されるとは限らない。そこで、信用できる機関が広告配送サービスを行う仲介することが考えられる。

【0076】図9における説明では、個人情報管理システムを信用できる機関として、個人情報管理システムで情報連携を行う例を記した。しかし、広告配送専用のサービスシステムB(例えば、SS-B)が信用できるか、またはSS-Bが利用条件を課せられた上でサービスを提供するならば、情報連携をSS-Bで行う方法も採ることができる。実現には、暗号・認証技術と、カプセル化等を用いた利用制御技術を用いた方法が考えられる。

【0077】SS-Bが該サービスを提供する場合、SS-Aは広告情報をカプセル化し、広告情報の内容だけでなくSS-Aが発信者であることも掌握できないような利用条件と共にSS-Bに送り、SS-Bは対応するユーザの個人情報から住所(電子メール広告の場合はメールアドレス)を調べ、関連付けることだけが可能な利用条件を課せられているが、該ユーザのもとに広告情報を配送することは実現できる。

【0078】

【発明の効果】以上述べたように、本発明では、ユーザがサービスシステム毎に用意した鍵ペア及びサービスシステムが発行した顧客IDを用いて匿名のまま顧客登録を行い、ユーザが顧客ID及び公開鍵を個人情報管理システムにのみ公開し、ユーザ個人情報として登録することで、個人情報管理システムを介することなく顧客認証を行うことができる。サービスシステムがユーザの身元確認を必要とする場合は、サービスシステムが個人情報管理システムに問い合わせることで匿名のまま身元証明を行うことができる。また、ユーザが匿名でサービスを受けるための識別情報をサービスシステム毎に個別に用意することで、複数のサービスシステムで格納されている個人情報を識別情報を用いて連携させ、ユーザが意図しない個人情報を作り出すという行為を制限することができる。

【図面の簡単な説明】

【図1】本発明の個人情報統合管理システムの実施の形態の一例を示す構成図

【図2】本システムの各構成要素に格納される個人情報の具体例を示す説明図

【図3】個人情報管理システムの概要を示す構成図

【図4】個人情報管理サービスの処理の流れ図

【図5】サービスシステムの概要を示す構成図

【図6】サービスシステムにおける提供サービスの処理の流れ図

【図7】個人情報管理システム及びサービスシステムの概要を示す構成図

【図8】個人情報管理システムとサービスシステムとの連携サービスの処理の流れ図

【図9】連携サービスの実現例を示す説明図

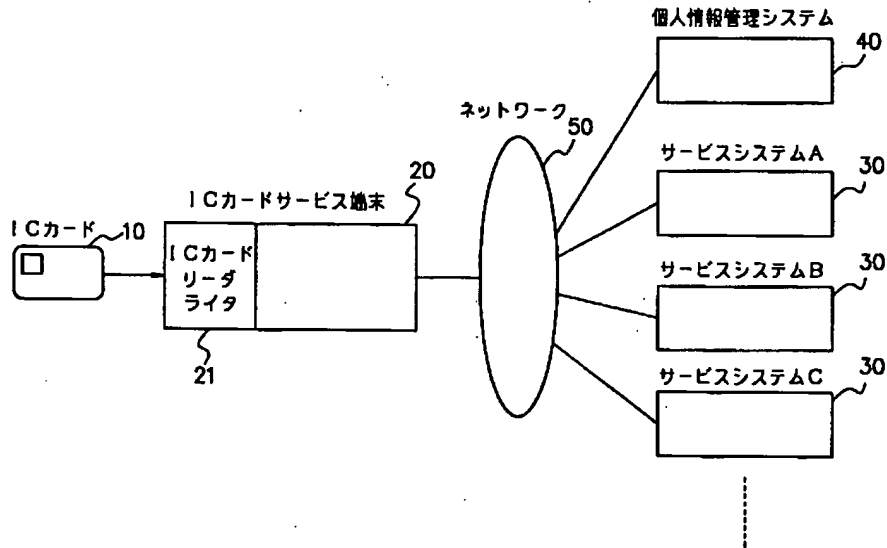
【符号の説明】

10:ICカード、11:カード用管理AP、12:力

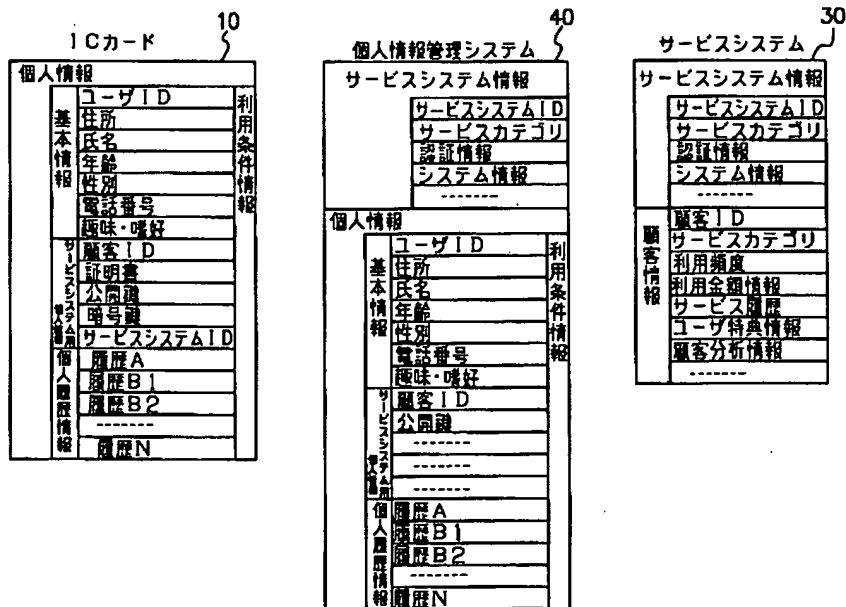
ード用サービスAP、20：ICカードサービス端末、
21：ICカードRW、22：端末用管理AP、23：
端末用サービスAP、30：サービスシステム、31：
サービスシステム顧客DB、32：サービス処理モジュ

ール、40：個人情報管理システム、41：個人情報D
B、42：サービスシステムDB、43：個人情報管理
モジュール、44：サービスシステム管理モジュール、
45：利用制御モジュール、50：ネットワーク。

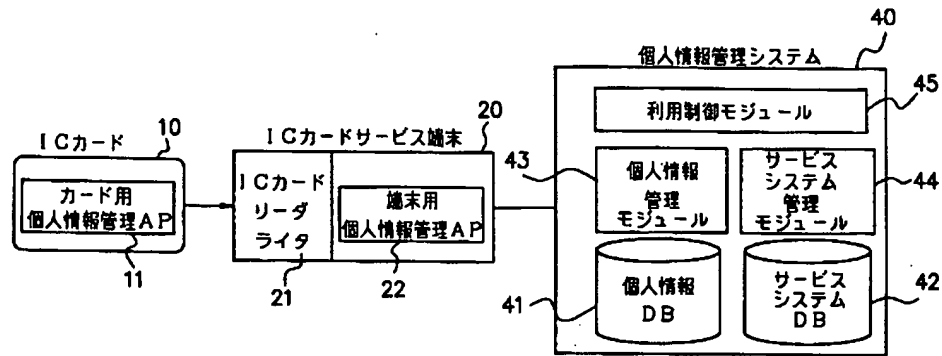
【図1】



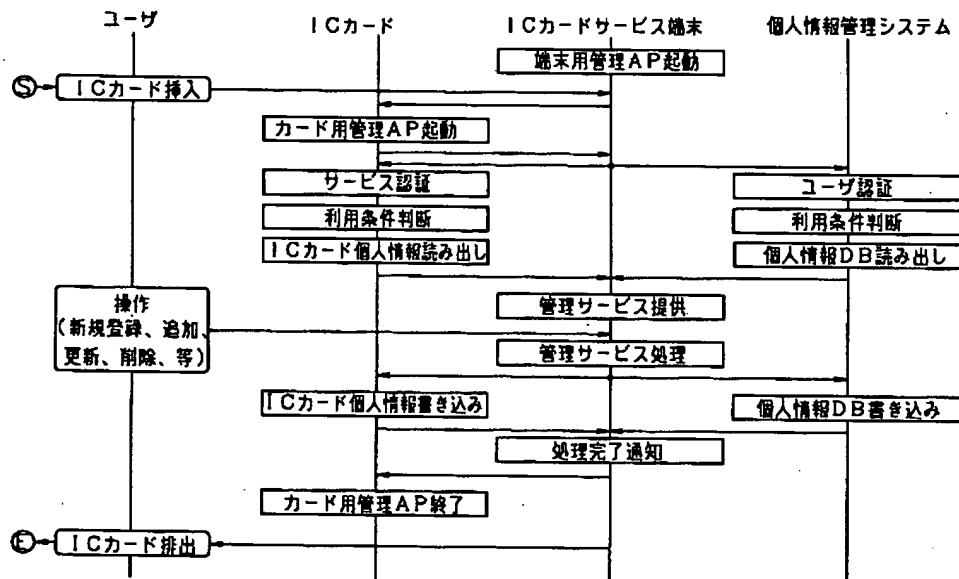
【図2】



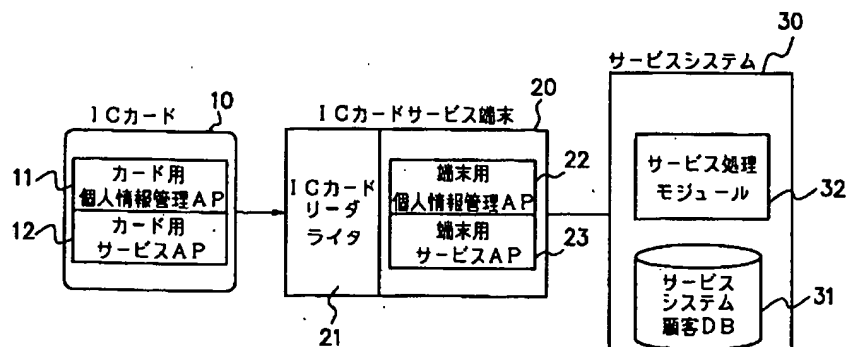
【図 3】



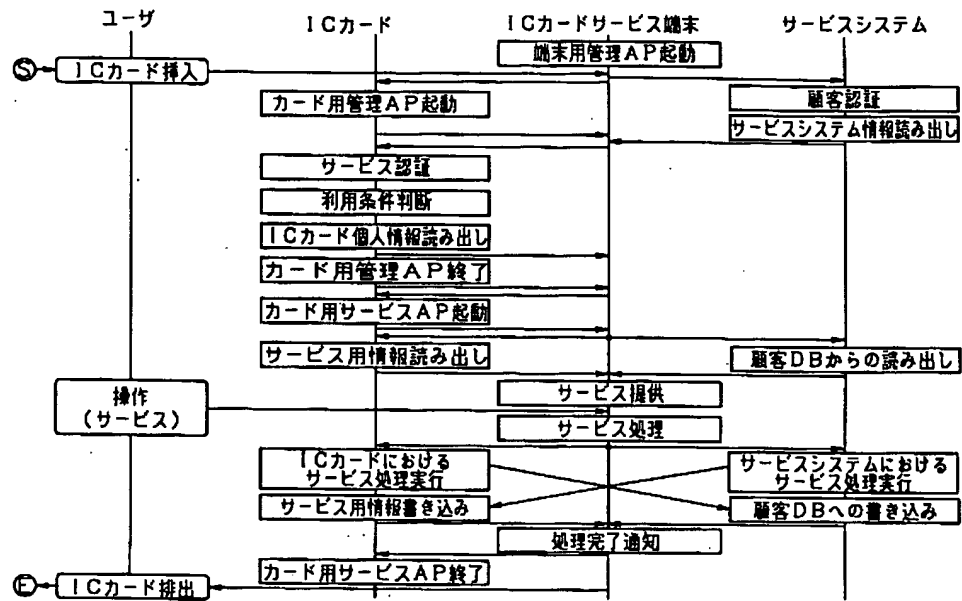
【図 4】



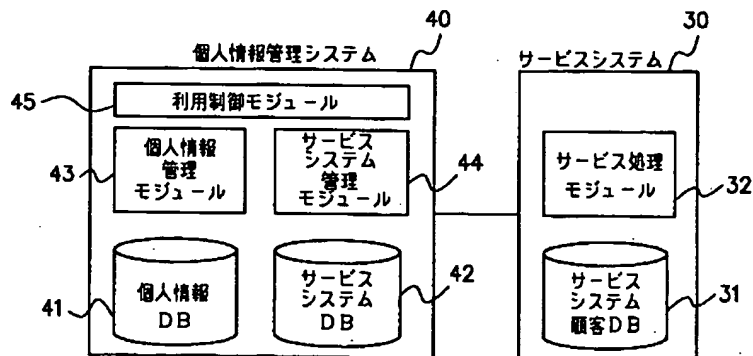
【図 5】



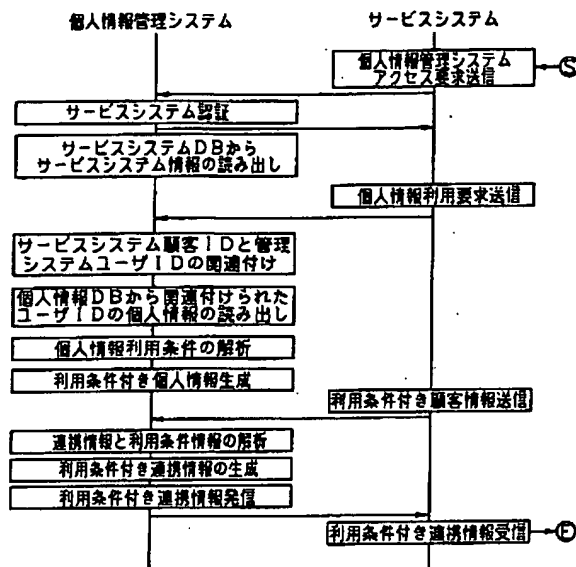
【図 6】



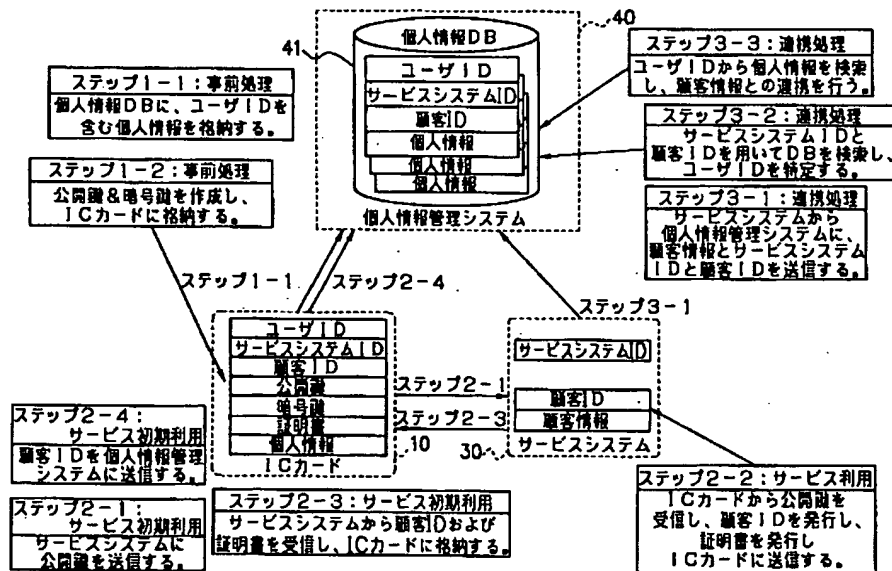
【図 7】



【図 8】



【図 9】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
15/00	330	15/00	330 G 5B085
17/30	170	17/30	170 Z
17/60	330	17/60	330
	510		510

(72)発明者 西田 玄

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

Fターム(参考) 2C005 MA04 MB01 MB08 MB10 NA02

SA02 SA06 SA12 SA13 SA22

SA25 SA30 TA21

5B017 AA03 BA05 CA14

5B058 CA25 KA02 KA04 KA08 KA31

KA35 YA20

5B075 KK02 ND20 UU08

5B082 EA12 JA08

5B085 AA08 AE01 AE06 AE12 AE23

BA07 BG07

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.